Ring Models for Group Candidates

William McCune

August 2004

`http://www.mcs.anl.gov/~mccune/projects/gtsax/`

Single Equational Axioms for Group Theory

In terms of division, $x/y = x \cdot y'$.

- Higman and Neumann, 1952:

$$x/((((x/x)/y)/z)/(((x/x)/x)/z)) = y.$$

  This has type (19,3). (Length 19 with 3 variables.)

  Is there a simpler one (in terms of division)?

  No.

  A nonassociative inverse loop (size 7) kills all nontrivial candidates.

In terms of product and inverse.

- Neumann (1981), type (20,4):

$$x \cdot (((y' \cdot (x' \cdot z))' \cdot u) \cdot (y \cdot u)')' = z.$$

- Kunen (1992), type (20,3):

$$((z \cdot (x \cdot y)')' \cdot (z \cdot y')) \cdot (y' \cdot y)' = x.$$

- McCune (1993), type (18,4):

$$y \cdot (z \cdot (((u \cdot u') \cdot (x \cdot z)') \cdot y))' = x.$$

- Kunen (1992) showed that the only possibility for a simpler axiom in terms of product and inverse is one of type (18,3).

Product/Inverse Candidates of Type (18,3)

- There are 20,568 candidates to start with.
- Collect a set of small countermodels by using Mace4.
- Tight constraints allow searces for larger countermodels.
  - nonassociative inverse loops (orders 10, 12, 16)
  - ring models

Ring Example

- Candidate

$$(((x \cdot y)' \cdot z) \cdot (((z \cdot z)' \cdot z) \cdot x))' = y.$$

- Consider the ring of integers mod 5, and let

$$\begin{aligned} &x \cdot y = 2x + y \\ &x' = 3x \end{aligned}$$

- The candidate is true in this structure, but “·” is not associative.
- Extend Mace4 to search for ring countermodels like this.

Mace4 Input File

```
% Fix [+,-,*] as the ring of integers (mod domain_size).
set(integer_ring).

clauses(theory).

% candidate
g(f(f(g(f(y,z)),x),f(f(g(f(x,x)),x),y))) = z.

% f and g in terms of the ring operations
g(x) = M * x.
f(x,y) = (H * x) + (K * y).

% denial of associativity
f(f(a,b),c) != f(a,f(b,c)).

end_of_list.
```

Mace4 Output

```
g(f(f(g(f(y,z)),x),f(f(g(f(x,x)),x),y))) = z.  % candidate

g(x) = M * x.
f(x,y) = (H * x) + (K * y).

f(f(a,b),c) != f(a,f(b,c)).  % denial of associativity

----------------------------------------------------------

M=3, H=2, K=1,
a=1, b=0, c=0,            f :   | 0 1 2 3 4
                              --+----------
g :     0 1 2 3 4             0 | 0 1 2 3 4
    -------------             1 | 2 3 4 0 1
        0 3 1 4 2             2 | 4 0 1 2 3
                              3 | 1 2 3 4 0
                              4 | 3 4 0 1 2
CPU time: 0.01 seconds.
```

Filter Summary

Model File	Models	In	Out	Killed
2-3	25	20568	3541	17027
nail-7	1	3541	2331	1210
nail-10	1	2331	1942	389
nail-12	1	1942	1784	158
nail-16	1	1784	1686	98
ring-4	5	1686	1354	332
ring-5	30	1354	955	399
ring-7	56	955	450	505
ring-9	9	450	420	30
ring-11	62	420	219	201
ring-13	8	219	183	36
ring-17	21	183	133	50
ring-19	6	133	116	17
ring-23	1	116	111	5
ring-29	2	111	43	68
ring-41	2	43	36	7

36 candidates remain (some can be proved from others)

1	$(((x \cdot x) \cdot y) \cdot ((x \cdot y)' \cdot (z \cdot x)'))' = z$	19	$x \cdot (((y \cdot (y \cdot y)') \cdot (x \cdot z')) \cdot z)' = y$
2	$((x \cdot x) \cdot y) \cdot ((x \cdot y)' \cdot (z' \cdot x)') = z$	20	$(x \cdot ((y \cdot ((x \cdot y)' \cdot (x \cdot z)')) \cdot x))' = z$
3	$(((x \cdot y)' \cdot z) \cdot (x \cdot ((z \cdot x)' \cdot x)))' = y$	21	$x \cdot ((y \cdot ((x \cdot y)' \cdot (x \cdot z')')) \cdot x) = z$
4	$((x \cdot y')' \cdot z) \cdot (x \cdot ((z \cdot x)' \cdot x)) = y$	22	$(x \cdot ((y \cdot (z \cdot x)') \cdot (z \cdot (x \cdot x)))')' = y$
5	$(x \cdot y)' \cdot ((((x \cdot x) \cdot y) \cdot z)' \cdot x)' = z$	23	$x \cdot ((y' \cdot (z \cdot x)') \cdot (z \cdot (x \cdot x)))' = y$
6	$(x' \cdot y) \cdot (((y \cdot (x \cdot z)') \cdot y)' \cdot y) = z$	24	$(x \cdot ((x' \cdot y) \cdot (((y \cdot z) \cdot y)' \cdot y)))' = z$
7	$(x' \cdot y) \cdot ((z \cdot (x \cdot (z \cdot z))') \cdot y)' = z$	25	$x \cdot ((x' \cdot y) \cdot (((y \cdot z') \cdot y)' \cdot y)) = z$
8	$((x \cdot y) \cdot ((z \cdot (x \cdot (z' \cdot z))) \cdot y)')' = z$	26	$x \cdot ((x' \cdot y) \cdot (y \cdot ((z \cdot y)' \cdot y))') = z$
9	$(x' \cdot y) \cdot (y \cdot (((x \cdot z) \cdot y)' \cdot y))' = z$	27	$(x \cdot ((y \cdot z) \cdot (x \cdot ((z \cdot x)' \cdot x)))')' = y$
10	$(x \cdot y)' \cdot (x \cdot (x \cdot ((y \cdot z) \cdot x))')' = z$	28	$x \cdot ((y' \cdot z) \cdot (x \cdot ((z \cdot x)' \cdot x)))' = y$
11	$x \cdot ((((y \cdot (y \cdot x)') \cdot y) \cdot z)' \cdot y)' = z$	29	$x \cdot ((y \cdot x)' \cdot (y \cdot (y \cdot (z \cdot y))')') = z$
12	$(x \cdot ((((x \cdot y) \cdot (x \cdot z')) \cdot z)' \cdot x))' = y$	30	$x \cdot (x \cdot (((y \cdot (x \cdot z')) \cdot z)' \cdot x))' = y$
13	$x \cdot ((((x \cdot y') \cdot (x \cdot z')) \cdot z)' \cdot x) = y$	31	$x \cdot (x \cdot (((y \cdot x)' \cdot (x \cdot z')) \cdot z))' = y$
14	$(x \cdot (((y \cdot ((y' \cdot x) \cdot z)) \cdot x)' \cdot x))' = z$	32	$(x \cdot (x \cdot ((y \cdot ((x \cdot y)' \cdot z)) \cdot x))')' = z$
15	$x \cdot (((y \cdot ((y' \cdot x) \cdot z')) \cdot x)' \cdot x) = z$	33	$x \cdot (x \cdot ((y \cdot ((x \cdot y)' \cdot z')) \cdot x))' = z$
16	$x \cdot ((((y \cdot x)' \cdot x)' \cdot (z \cdot x)') \cdot z) = y$	34	$(x \cdot (y \cdot (((x \cdot y)' \cdot z) \cdot (y \cdot z)')))' = y$
17	$(x \cdot ((((x \cdot y) \cdot x)' \cdot (x \cdot z')) \cdot z))' = y$	35	$x \cdot (y \cdot (((x \cdot y)' \cdot z) \cdot (y' \cdot z)')) = y$
18	$x \cdot ((((x \cdot y') \cdot x)' \cdot (x \cdot z')) \cdot z) = y$	36	$x \cdot (y \cdot ((y' \cdot x) \cdot ((z \cdot x)' \cdot x)))' = z$